

Keycafe Security Architecture Overview

Introduction

Keycafe provides a convenient way for businesses to remotely manage keys while maintaining an acceptable security level for most use cases. From product design to systems architecture to solid SmartBox construction, our solutions are designed from the ground up with a balance of security, convenience and usability in mind. This overview describes the essential security features built into the Keycafe Smart Key Management platform.



Best-In-Class Server, Application & Database Architecture

State-of-the-art service & security

Keycafe integrates with best-in-class software providers to offer top level security on the back end. Transport Layer Security, Denial of Service attack protection, and Managed Firewalls are integral to our data server architecture. Keycafe observes security best practices such as password hashes, access logging, source code reviews and penetration testing.



Transport Layer Security

TLS encrypts, authenticates, and verifies data integrity against tampering. A private communication channel between your computer and Keycafe ensures that when you manage your account, all information is safely transmitted.



Denial of Service

Access to Keycafe is secured against Denial of Service (DDOS) attacks by a best-in-class CDN partner. With over 67 Tbps of network capacity, Cloudflare blocks an average of 70B threats per day to protect you against the largest and most sophisticated attacks.



Managed Firewalls

Your data is secure behind multiple state-of-the-art firewalls. Firewalls are fundamental to protecting network traffic including the flow of sensitive data. They are required for compliance to mandates like PCI DSS, HIPAA, and GDPR.



PCI Compliant Payment Processing

Your payment information is encrypted by a PCI compliant payment processor certified to PCI Service Provider Level 1, the most stringent level of certification available in the payments industry.



Penetration Testing

Keycafe periodically performs automated penetration testing to find vulnerabilities before they can be exploited. These tests, designed by security experts, simulate the activities of real hackers to flag issues like misconfigured servers, SQL injection, cross-site scripting, exposed files/directories, weak encryption protocols or cyphers, and many others. They also test for known vulnerabilities in popular software and protocols ("Heartbleed", etc.).

Our software suppliers equip Keycafe with constant, industry leading threat monitoring and automatic OS vulnerability patching. Selected Keycafe software providers include:



Cloudflare

World leader in DDoS protection, rate limiting, proxy for CDN performance improvements, and DNS management. Cloudflare is trusted by 25M internet properties.



Heroku

Highly advanced security for web hosting, systems administration, Linux security updates, database security updates, firewall, and software intrusion detection. Heroku is ISO 27001, 27017, 27108 compliant with SOC 1, 2, 3 reporting. [See more.](#)



Hologram

Provides advanced and customizable cellular IoT connectivity to reliably launch, scale, and secure global device fleets.



Intruder.io

Intruder is a cloud-based vulnerability scanner that finds cyber security weaknesses in digital infrastructure.

Keycafe is scanned daily by Intruder.io for resistance against 10,000 attack vectors with an A+ rating.



Stripe

The leading online billing platform. Millions of businesses of all sizes—from startups to large enterprises—use Stripe’s PCI compliant software and APIs to accept payments, send payouts, and manage their businesses online.

Service Level Agreement



99.9% uptime guarantee. [Read more](#)

Compliance and Continuous Monitoring

Keycafe uses Drata to automate and monitor compliance with SOC 2, GDPR, and related privacy and security frameworks. Keycafe has completed a SOC 2 Type I audit confirming that our controls meet the trust service criteria for security, availability, and confidentiality. Drata provides real-time oversight of control status and ensures our systems and policies remain audit-ready. Customers can view certifications and reports through the [Keycafe Trust Center](#).



Privacy Policy & Data Processing

GDPR compliant

The Keycafe [Privacy Policy](#) outlines what information is collected and how it is used, shared, secured, and stored. Keycafe is based in Vancouver, Canada, and customer data is processed and stored by trusted third-party cloud providers with GDPR compliance programs. These providers operate under data processing agreements that define how customer information is managed.

Keycafe's [Data Processing Addendum](#) has been recently updated to reflect current privacy standards and outlines how customer data is protected in accordance with applicable regulations.

User Authentications & Permissions

Tailored access authentication

Keycafe user authentication offers a number of options to give you control over who accesses your business's key to rental properties, vehicles, and company facilities. As a default setting, two factor authentication is enabled requiring end users to input an ID number plus an access code sent via SMS message.

Depending on your subscription plan, a variety of additional custom permissions can be layered in for authentication, such as administrative controls, scheduled permissions, badge scans, and more. Utilizing the full breadth of our user-facing authentication options and tailoring access to each user of your SmartBoxes is an important deterrent to unauthorized access to keys.

Below is a table of the types of objects that can be accessed and the permissions options that can be granted and managed.



keycafe

Object / Permission Type	Description	Who Can Access	Authentication Requirement
Key Codes	A simple code that can be created for any key which when entered at the SmartBox, reveals the key. The key code is valid until withdrawn.	Any person you give the key code to	Inputting the key code on the SmartBox
Scheduled Bookings	An access to a key that is valid within a specific time frame where the party is not required to be a registered user.	Any person you give the booking details to	Entering the booking code at the SmartBox or utilizing the unique URL for the mobile friendly experience.
Single Key Permission	A permission in the database for a user or group of users to access a specific key.	Any user given exchange or admin permissions to the key, or any user in a group of users that has exchange or admin permissions to the key	Using Keycafe iOS or Android App, or entering ID code at SmartBox plus 2FA code if required by settings
All Keys Permission	A permission in the database for a user or group of users to access all keys owned by your account.	Any user given exchange or admin permissions to the all keys group, or any user in a group of users that has exchange or admin permissions to the all keys group	Using Keycafe iOS or Android App, or entering ID code at SmartBox plus 2FA code if required by settings.
Custom Group of Keys	A permission in the database for a user or group of users to access a group of keys you have designated.	Any user given exchange permissions, User given admin permissions to the custom key group, group of users with exchange or admin permissions to the custom key group	Using Keycafe iOS or Android App, or entering ID code at SmartBox plus 2FA code if required by settings.
Key Bin	An ability for a user to remotely open any key bin on the SmartBox regardless of key permissions.	Any user given admin permissions to the key exchange location	Using Keycafe web app, iOS or Android App.
SmartBox Main Lock	An ability for a user to remotely unlock from the wall the entire SmartBox regardless of key permissions	Any user given admin permissions to the key exchange location	Using Keycafe web app, iOS or Android App.

IoT Server to SmartBox Communication

Robust, dynamic & informative

By integrating with Particle's Device Cloud, Keycafe IoT security is backed by best-in-class hosting with ISO 27001, 27017, and 27018 physical security and risk management which minimizes attack surface area in both the service layer and data.



Advanced IoT Security

All communication between the SmartBox and our servers is encrypted and secure. Leaving no incoming ports open, our service thwarts port scanners and side attacks. Each device carries a unique encryption key, and continuous security landscape monitoring protects servers from potential threats.



Encrypted Radio Connections

BLE communication with the SmartBox is fully encrypted in transit. WiFi connections are secured using WPA2, the industry standard. Cellular connections use industry standard encryption to ensure all data is safe in transit.



Device Activity Alerts

With 24/7 SmartBox cloud connectivity, key exchanges automatically trigger detailed notifications in real time via email, mobile notifications, or webhook. Since authentication occurs live in communication with our server, Keycafe provides real-time control over access to your keys.



OTA Updates

Each SmartBox receives over the air updates which means firmware and security features are always up to date to stay one step ahead of emerging threats.

SmartBox Construction

Solid construction and tamper resistance

Our steel plate mounted SmartBox features a rugged 16 gauge powder-coated steel frame. Inside, each individual key bin is constructed with a separate die cast metal door enclosure. The electronic master lock is inaccessible and fully hidden from view. The SmartBox is designed to deter most opportunistic tampering and misuse given its solid metal construction, locks on each individual key bin, and lack of any externally facing master lock. We offer an outdoor steel enclosure accessory with a loop for a lock which can be used for additional security with outdoor placements.

Not a safe

The Keycafe SmartBox is not a safe and not designed or rated to resist determined theft or equipped to prevent relay/replay, cloning, or signal amplification attacks. Even rated safes in practice can resist determined theft for only a limited period of time. Our product is designed to provide usability, convenience and security by way of enhanced trackability and accountability. The SmartBox should only be used in well lit, surveilled environments you believe unlikely to attract theft. You should check with your insurance provider concerning how use and placement of the SmartBox may impact any claims. You must exercise judgment as to whether the convenience of automated and unsupervised key exchange is appropriate for your use case and needs. Please see the Keycafe Terms of Service for additional security advisories.



SmartBox Features:

- 16-gauge steel plate wall mount
- Precision molded polycarbonate frame with 20-gauge steel reinforcements
- A383 alloy diecast metal doors
- Built-in video surveillance options
- Inaccessible, electronically controlled master access
- Weather resistant powder coating
- Additional outdoor steel enclosure option

Each SmartBox is further protected by state-of-the-art IoT security, customizable authentication workflows, and best-in-class software integrations as described above.

Further Information

While our support and sales teams do their best to communicate on a broad array of technical topics related to our products, their answers may not always be fully nuanced or up to date. This document provides a high level summary of our security architecture, practices and key vendors. If you have a security question not addressed by this document and require a definitive answer, please reach out to security@keycafe.com and we will consult our product leaders and engineers to provide you with additional information.